MINUTES
of the
THIRD MEETING
of the
INFORMATION TECHNOLOGY OVERSIGHT COMMITTEE

July 27, 2005
Macey Center, New Mexico Institute of Mining and Technology, Socorro

The third meeting of the Information Technology (IT) Oversight Committee for the 2005 interim was called to order by Senator John Arthur Smith, vice chair, on July 27, 2005 at 9:40 a.m. in Socorro at the Macey Center of the New Mexico Institute of Mining and Technology (New Mexico Tech).

Present
Sen. John Arthur Smith, Vice Chair
Rep. Janice E. Arnold-Jones
Sen. Vernon D. Asbill
Sen. Linda M. Lopez
Sen. Richard C. Martinez
Rep. Thomas C. Taylor
Rep. Luciano "Lucky" Varela

Absent
Rep. Debbie A. Rodella, Chair
Sen. William H. Payne
Rep. Richard D. Vigil

Advisory Members
Sen. Rod Adair
Rep. Justine Fox-Young
Sen. Phil A. Griego
Rep. Jeannette O. Wallace

Sen. Mark Boitano
Sen. Pete Campos
Rep. Richard P. Cheney
Sen. Carlos R. Cisneros
Rep. Ted Hobbs
Sen. Gerald Ortiz y Pino

Staff
Raul E. Burciaga
Ralph Vincent
Amy Chavez

Guests

The guest list is in the meeting file.

Copies of all handouts and written testimony are in the meeting file.

Approval of Minutes

On motion duly made, seconded and adopted without objection, the committee approved the minutes from its last meeting held on June 30 in Santa Fe.

Introductory Remarks

Dr. Daniel H. Lopez, president, New Mexico Tech, welcomed members of the committee to Socorro and to the New Mexico Tech campus. He discussed New Mexico Tech's involvement in research for the Institute for Complex Additive Systems Analysis (ICASA) and explained the project's significance to federal government security. He also discussed projects benefiting state government, including assistance to the Commission on Higher Education in tracking student identification numbers.

Information Assurance Research at New Mexico Tech

Dr. Andrew Sung, professor and chair of the Computer Science Department at New Mexico Tech, discussed various information assurance research initiatives undertaken at the institute. As part of the Center for Academic Excellence/Information Assurance Education (CAE/IAE) Program, faculty and students have conducted projects on information assurance development. Dr. Sung explained New Mexico Tech's role in offering information assurance training, workshops and tutorials to students and government clients.

Steganography was noted as among the leading areas of information assurance research and training at New Mexico Tech. Steganography is the study of the use of combined media that form codified messages for communication. Dr. Sung noted that terrorist organizations and other threats to national security might use steganography as a communication tool. New Mexico Tech faculty and students are in the process of conducting steganalyses to learn how to detect and decode steganographic messages. The steganalyses involve the use of feature selection to distinguish inconsistencies in digital data to identify the presence of steganographic messages. Dr. Sung explained that the studies will aid in the future detection of possible information security risks such as unauthorized probing, surveillance and access to information by unauthorized parties.

Patrick Chavez and Sandeep Mandada, New Mexico Tech doctoral students, provided summaries of their information assurance graduate research projects. Mr. Chavez is conducting research on paradigm shifts in information assurance and Mr. Mandada is studying the possibility of the use of consolidated passwords for protection of classified information.

L.M. Liebrock, administrator of the Scholarship for Service Program under the CAE/IAE Program, discussed the variety of information assurance-related projects developed by New Mexico Tech students participating in the scholarship program. The program's scholarship recipients are required to complete research projects in the field of information assurance. Program participant projects include research on subjects such as virtual local access network virus containment, wireless sensor network security, spyware detection, grid security infrastructure, digital forensics and usable security policy.

System Engineering Security

Dr. Pradeep K. Kholsa, dean of the College of Engineering at Carnegie Mellon University, provided the committee with an overview of the threats and risks that exist with respect to information security in the United States. Dr. Kholsa explained that increased

numbers of internet users and providers have exposed information systems to more significant threats than existed in the 1980s. As technological improvements in microprocessor chips, storage densities and bandwidths have arisen, virus propagation rates have increased. In 2001, for instance, 80,000 network intrusion attacks were reported. Such incidents have risen exponentially and the nature and location of such attacks remains unpredictable. Unpredictability exists because attacks on systems do not require complex knowledge on the part of hackers and other system attack culprits. Adding to the problem is that today's information technology environment is characterized by open, highly distributed systems; unknown perimeters, components and participants; and a lack of central, administrative control. Dr. Kholsa predicted that future attacks might occur quickly enough so that human response to attacks will be impossible.

Vulnerabilities in information technology systems could have significant adverse effects upon the national economy. During the 1990s, two-thirds of productivity in the United States was attributed to the use of information technology. Attacks on information systems could negatively impact banking systems and could contribute to business losses and failures in market mechanisms. Government information systems, critical infrastructure power grids, water systems and air traffic might also be disrupted.

Dr. Kholsa warned that international terrorists are not the only threats to information system security in the United States. Many of the biggest threats to information system security come from within the country. Organized criminals, disgruntled employees, hackers, business competitors and other governments account for more than 50 percent of information system attacks. When information security is breached, consequences include disclosure of customer records, operation sabotage, trade secret theft and electronic fund transaction fraud. Ultimately, business and governments might suffer a loss in citizen and client confidence. Legal liability might also result.

Dr. Kholsa described the work of CyLab, the nation's largest program focused on cybersecurity and on the dependability and privacy of information systems. The mission of CyLab is to conduct research and development and provide education to increase information system security. CyLab is currently working on a project to develop self-securing devices that protect computers and network environments. Other CyLab projects are focused on the development of virus propagation models, human-centered security interfaces and secure information storage systems that permit disbursement of information throughout cyberspace networks. CyLab has also led to initiatives that inform network users of possible risks to information security.

According to Dr. Kholsa, the information system security market is predicted to expand significantly during the next few years. In 2004, that market generated $20 billion to $25 billion in the United States and is expected to increase to $50 billion by 2008.

ICASA Methodology

Steven Ball, senior researcher with the department of Electrical Engineering at New

Mexico Tech, provided the committee with an overview of the work of ICASA. The institute is based within the Energetic Materials Research and Testing Center (EMRTC) of New Mexico Tech. Mr. Ball explained that ICASA conducts research to understand the behavior of critical infrastructure systems and vulnerabilities that are of interest to national security. The institute conducts operational vulnerability and informational vulnerability assessments to expose methods in which information systems might be exploited. The institute also uses computer models to expose abnormalities in information security systems.

Energetic Materials Research and Testing Center

Representatives of the EMRTC for New Mexico Tech provided a summary of the center's efforts in exploring methods of national physical security. New Mexico Tech owns 40 miles of test area, on which the center tests explosives as part of the federal Department of Homeland Security's research and development efforts. The center has also developed a countermine test site, used for research in the detection of antitank and antipersonnel mines. Such research has been used to aid United States troops in Iraq. The EMRTC also hosts training programs on incident response to terrorist bombings, antiterrorism assistance and explosives safety. Many of these training programs are held in Playas, New Mexico, which was purchased by New Mexico Tech. Real-time terrorist attack and security incident scenarios take place in Playas as part of training initiatives to educate various entities to respond to such attacks and incidents in small-town settings.

Office of Homeland Security

Tim Manning, acting director, Office of Homeland Security, discussed the efforts of the office to ensure information security in the state. The office has established a terrorism risk assessment program, composed of representatives from various agencies, to analyze risks on state-owned facilities. Analyses are conducted on the basis of a prioritized list developed by the program.

Mr. Manning further updated the committee on his efforts to work with the federal Department of Homeland Security and with various utilities to protect infrastructure networks. He mentioned that some responsibilities will be transferred to the Office of the Chief Information Officer. Committee members asked Mr. Manning to provide accountings of appropriations received by the Office of Homeland Security from the New Mexico Legislature and the federal government.

Status of Information Technology (IT) Initiatives

Aurora Sanchez, IT performance auditor, provided the committee with a status report of the findings of the Legislative Finance Committee (LFC) with respect to IT audits of the Office of Workforce Training and Development (OWTD) and the Labor Department (LD). The LFC conducted an audit on the virtual one-stop system (VOSS) developed by the OWTD. Ms. Sanchez explained that the system is a common intake system designed to be used by various agencies that provide work and training services to New Mexicans. The LFC found as a result of its audit that the OWTD and LD lack a good working relationship. Ms. Sanchez further predicted that moving the VOSS application to the General Services Department from the vendor

site before establishing a good working relationship might adversely affect both agencies.

The LFC also conducted an audit of the unemployment insurance claims system of the LD. The system is used to assist the LD in establishing unemployment claims; providing benefit payments to eligible claimants; filing claims appeals; and measuring quality and performance. As a result of the audit, the LFC discovered that good progress in project management reporting occurred and that necessary technical positions were being filled. However, the LFC also found that a contract with the unemployment insurance claims system had not been signed. The LFC recommends that project costs should be reconciled on a monthly basis and that training should be held for IT staff when existing technical position vacancies are full.

Ms. Sanchez additionally provided the committee with an update of the LFC's quarterly report on state agency IT projects. Data for two projects, E-911 and PERA-RIO, have been validated. Exit conferences with the agencies responsible for the projects will be scheduled. In general, report data indicates that agencies are prone to either overstate or understate project costs and incorrectly report project appropriations. Ms. Sanchez suggested that quality control reporting has also lacked important information indicating the acceptability of software and deliverables. The report further indicates that project schedules are not adequately maintained by project managers.

IT Commission Update

Carroll Cagle, chair of the IT Commission, discussed the priorities of the IT Commission, including consolidation, cybersecurity and project management. He indicated that the committee is focused on an increased volume of projects. He also discussed changes in the composition of the commission, including the introduction of Estevan Gonzales and David Horking, two new commission members.

Office of Chief Information Officer (CIO) Update

Ray Soto, state CIO, expressed approval of the quarterly report of state agency IT projects generated by the LFC. He stated that agencies have been cooperative in the reporting process and that all agencies reported in June. He further indicated that random audits of the agencies by the LFC in addition to the possible need to report to the IT Commission have provided agencies with incentives to cooperate with the CIO and the LFC.

Mr. Soto also discussed the recent hiring of a general counsel to review IT contracts on behalf of the CIO. The CIO will publish a contract guidance manual to assist agencies in using the necessary technical and legal information to negotiate IT contracts.

The committee adjourned at 4:35 p.m.